

Before you point AI at client data: a governance checklist

For bookkeepers and BAS agents. Work through every box before any client data goes near an AI tool, then review it whenever you add a new tool or a new team member. If you can't tick a box, you're not ready yet.

1. Know where the data goes

- ☐ **Business plan, not personal.** Every AI tool that touches client data is on a business or team account, never a staff member's personal login.
- ☐ **Training confirmed.** You've checked in the provider's current terms whether your data is used to train their models, and you're comfortable with the answer.
- ☐ **Location known.** You know where the provider stores and processes your data, including whether it leaves Australia.
- ☐ **Client permission in writing.** Under TPB Code item 6, externally hosted software is a third party. Your engagement letter, or a separate written consent, tells clients which AI tools and providers you use, and they've agreed.
- ☐ **Privacy policy current.** If the Privacy Act applies to your practice, your privacy policy reflects your AI tools, including any overseas disclosure.
- ☐ **No copy and paste.** Your team knows the rule: no client reports, ledgers or payslips pasted into any AI tool that isn't on the approved list.

2. The AI sees what the person sees

- ☐ **Own logins only.** Every person connects their own AI account with their own credentials. No shared logins, no shared connections.
- ☐ **Access follows the person.** A team member's AI can only reach the clients that person is allowed to work on.
- ☐ **Approved tools list.** You've written down which AI tools and connections (MCPs) the practice allows, and everyone knows where to find the list.
- ☐ **Audit trail.** You can see who asked what, which client data was accessed, and when.
- ☐ **Offboarding covered.** When someone leaves, their AI connections are revoked the same day as their other access.

3. Proposed, not posted

- ☐ **A person approves every change.** AI can find, flag and suggest. Nothing is posted to a client's ledger, lodged or sent to a client until someone reviews it and approves it.
- ☐ **Reasonable care stays with you.** Your team understands that the TPB Code's reasonable care obligations sit with the registered agent, not the tool. AI output is a draft until it's reviewed.
- ☐ **Evidence of review.** Your working papers show what was checked, what was found, what was changed, and who approved it.
- ☐ **Check it before you ask it.** Before relying on an AI answer about a client, you know the data underneath has been reconciled and checked.
- ☐ **Spot-check the answers.** Someone regularly traces AI answers back to source documents, especially figures headed for a BAS, an IAS or a client.